



**Law Enforcement Technical Forum
Fredericksburg, Virginia
March 5-6, 2013**

Administrative Matters/Welcome

- [redacted] *Supervisory Special Agent, CIU, FBI*
- [redacted] welcomed everyone to the Law Enforcement Technical Forum (LETF) Conference and asked attendees to introduce themselves to the group.
 - A special "thank you" was given to [redacted] for coordinating the event.
 - Travel vouchers are due by March 12, 2013.
 - [redacted] introduced SSA [redacted] liaison representative.

b6
b7C

Welcome/Update of the FBI's National Domestic Communications Assistance Center (NDCAC)

- [redacted] *NDCAC, FBI*
- [redacted] welcomed the group and provided an overview of the NDCAC and its recent relocation to Fredericksburg, Virginia. She introduced the NDCAC staff present at the meeting and briefly described the roles each would be filling at the NDCAC.
- [redacted] will lead the Technology Sharing function,
 - [redacted] is responsible for Training provided by the NDCAC and leveraging the training of other agencies on behalf of the NDCAC,
 - [redacted] will lead the Help Desk in providing 24/7 support to the law enforcement community,
 - [redacted] group of the NDCAC and is currently working on such issues as [redacted]
 - [redacted] is the NDCAC's law enforcement liaison representative,
 - [redacted] and [redacted] both from the [redacted] [redacted] are also contributing to various NDCAC initiatives.
- [redacted] described the recently complete [redacted]
 - [redacted] also mentioned that the AskCALEA website is expected to be operational again in June 2013.

b6
b7C

b6
b7C
b7E

Agenda

- **Administrative Matters/Welcome**
SSA [redacted] *Supervisory Special Agent, CIU, CIS, OTD, FBI*
- **Welcome Remarks and NDCAC Update**
SC [redacted] *CI, OTD, FBI*
UC [redacted] *NDCAC, OTD, FBI*
- **Regional Computer Forensic Lab (RCFL) Unit**
UC [redacted] *RCFL Unit, [redacted] OTD, FBI*
- **Technology Trends**

b6
b7C
b7E

Steve L. Stoner, Department of Defense

b6
b7C
b7E
b4

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] FBI
- [REDACTED] Town Hall Meeting
- [REDACTED] CIS, OTD, FBI
- National Computer Forensics Institute
- [REDACTED] Director NCFI, USSS
- [REDACTED]
- SSA [REDACTED] CID, FBI
- National Domestic Communications Assistance Center (NDCAC) Tour
- DAD Tony DiClemente, OTD, FBI
- [REDACTED]
- SSA [REDACTED] NDCAC, OTD, FBI
- [REDACTED] NDCAC, OTD, FBI
- [REDACTED] NDCAC, OTD, FBI
- [REDACTED] NDCAC, OTD, FBI
- [REDACTED] NDCAC, OTD, FBI

b6 Per USSS
b7C

b6
b7C
b7E

Welcome Remarks

SC William Searcy, CI, OTD, FBI

- SC Searcy provided brief remarks on the importance of State and local law enforcement outreach and how cooperation and coordination of efforts improves the chances of success.
- SC Searcy identified a potential issue with the upcoming conference in San Antonio. Budget related concerns may impact the conference. Going forward [REDACTED]

b7E

Regional Computer Forensic Lab (RCFL) Unit

UC [REDACTED] RCFL Unit, DES, OTD, FBI

- [REDACTED] provided LETF members a detailed description / introduction of the roles and support functions provided by RCFLs.
- An RCFL is a digital forensics laboratory and training center devoted to the examination of digital evidence in support of criminal investigations and to the detection and prevention of terrorist acts. The first RCFL was established in San Diego, California in 1999, and began as a cooperative effort between the FBI and other Federal, State, and local law enforcement agencies to address digital evidence. The RCFL Program is based on this model of partnership between the FBI and other law enforcement agencies at the Federal, State, and local levels operating within a geographic area.
- In addition to the San Diego RCFL, RCFLs are operating in Albuquerque, New Mexico; Buffalo, New York; Chicago, Illinois; Dallas, Texas; Dayton, Ohio; Denver, Colorado; Hamilton, New Jersey; Houston, Texas; Kansas City, Missouri; Louisville, Kentucky; Menlo Park, California; Orange, California; Philadelphia, Pennsylvania; Portland, Oregon; and Salt Lake City, Utah.

b6
b7C

- [redacted] identified the key goals of the RCFL Program:
 - Provide timely, professional and technically advanced digital forensic services to the law enforcement agencies in an RCFL's service area.
 - Fully utilize applied science and engineering capabilities to support digital forensic examinations.
 - Increase confidence of investigators, prosecutors, and judges in the digital forensics examination discipline through standardized training and forensic protocols.
 - Provide responsive and flexible services in support of diverse investigative programs.
 - Meet legal and administrative requirements of diverse judicial systems.
- [redacted] provided the group with a number of illustrative handouts and other guides:

b6
b7C

- [redacted]
- [redacted]
- [redacted]

b7E

Technology Trends

Steve Stoner, Department of Defense

- Mr. Stoner began by stating that the presentation would focus on emerging challenges with mobile access to the Internet and how is law enforcement affected by changes in mobility
- According to Mr. Stoner, mobility introduced the Internet to subscribers; mobility changes everything.
- By 2020, there will be 50 billion connections – seven for every person on the planet.
- The number of connected people is greater than the number of people who can read.
- The world is becoming saturated with cell phones – nearly 100 percent of the adult population in the U.S. owns a cell phone.
- 70 percent of new phones in the US are smartphones.
- Worldwide, smartphones account for 18 percent of the phones, but 90 percent of the data transferred.
- In 2012 the average user transferred 340 Mb/month. In 2017, it is projected to reach 2.16Gb/month.
- Previously, mobile operators added subscribers for growth but that approach is no longer a viable option.
- Wireless devices generate a large demand for data.
- Wi-Fi offload will become an increasingly used option.
- Video downloads and videoconferencing have become the norm.
- Data is doubling every year. This is forcing mobile operators to switch the core revenue generator from voice to data. Capital expenditure (CAPEX) is required to prevent churn.
- There is a lot of digital information available, making it easy to access content. Mobile devices allow users to be connected anywhere, anytime.
- Radio Interface Technologies (RITs) include:
 - 3GPP: High Speed Packet Access (HSPA), HSPA+
 - 3GPP: Long Term Evolution (LTE), LTE-Advanced
- Mr. Stoner showed a chart outlining the evolution of Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), and Orthogonal Frequency-Division Multiple Access (OFDMA) systems.
- The HSPA revolution has allowed for a six-fold increase in data rate growth. There are

multiple technology choices that can grow data capacity.

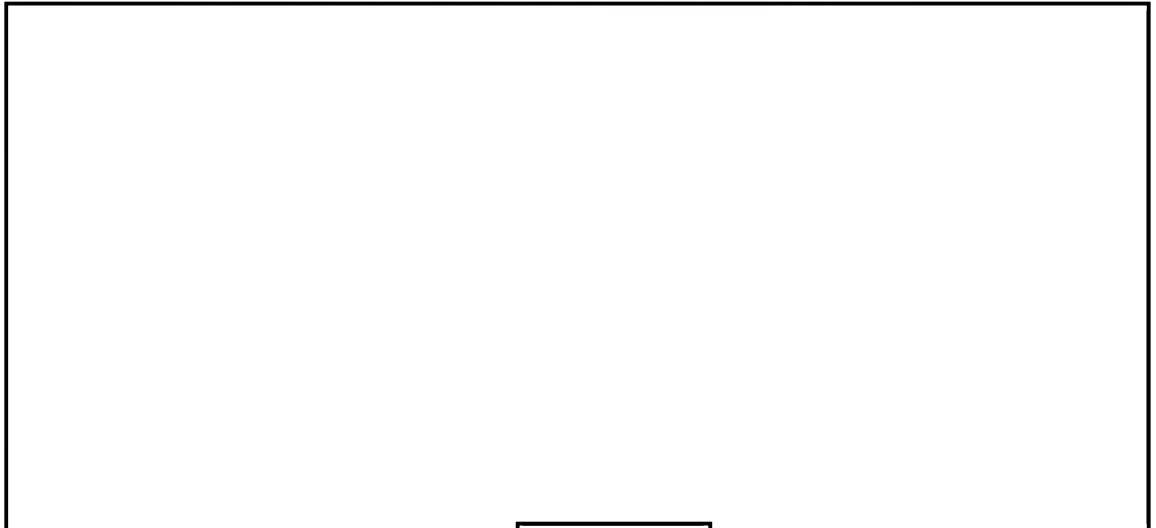
- LTE offers lower costs per bit of data. To obtain the benefits of LTE, it needs to be at a minimum of 10 megahertz (MHz); otherwise, the technology is not much better than HSPA+.
- Demand for data is outstripping improvements in technology. Operators are mitigating this issue with data tiered pricing.
- The price of smartphones is decreasing, which is resulting in an increase in the number of subscribers.
- The Internet is going mobile and applications like Google Maps provide a lot of access to information.
- There have been approximately 10 billion Apple app downloads since 2007. There are over 100 app stores. Writing a custom app is simple and can be done by almost anyone.
- Google is switching to mobile and is on the cusp of knowing everything about everyone.
- The first 10 years of the 21st century were used to digitize the world. The next 10 years will be about enhancing the world with digital information.
- The mobile Internet era may render mobile operators to dumb pipes.
- As a result of the increase in new mobile technologies, theft is going mobile.
- The plan is to connect everything in our lives—entertainment, retail, medical, work, and school.
- What do these changes mean for the law enforcement? How can social media be used successfully?
 - Traditional media (not searchable) vs. mobile Internet (searchable)
 - Crowdsourcing – act of outsourcing tasks, traditionally performed by an employee or contractor, to an undefined, large group of people or a community through an open call. Increasingly used for cost efficiency
 - Social media investigations – forensics, public assistance, and detection searches
 - Video surveillance - used to spot a missing child or a terrorist
 - Crime mapping – setup by people in their own communities
- Why use social media?
 - Community outreach and information
 - Cyber vetting
 - Entrepreneurs are establishing an online presence
 - Provides a direct relationship with the public
 - Tip lines
- Social media can reposition the relationship of police departments in their respective communities.

[redacted]
[redacted]
[redacted] provided an overview [redacted]
○ [redacted]
○ [redacted]
○ [redacted]

b6
b7C
b7E

b4
b7E

-
-
-
-
-
-
-
-

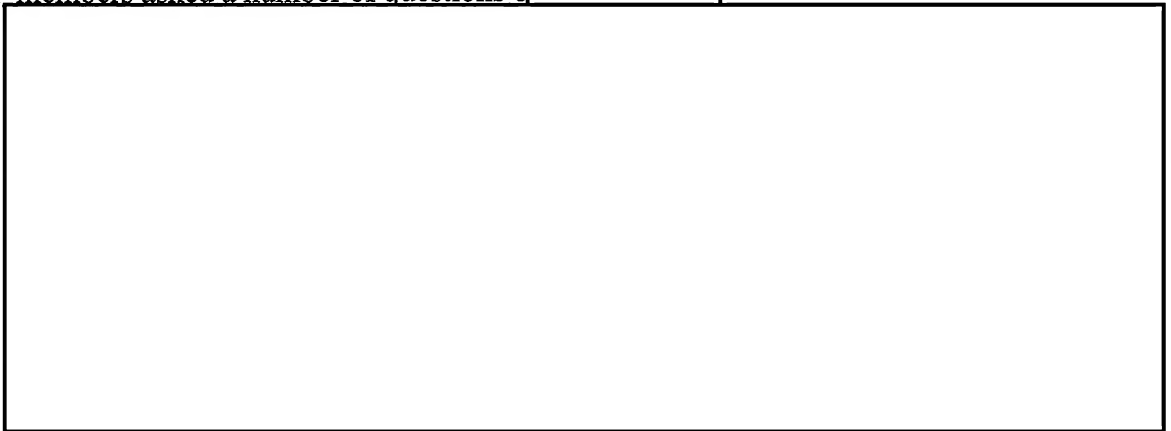


b4
b7E

- LETF members asked a number of questions of [redacted]

b6
b7C

-
-
-
-
-
-
-
-

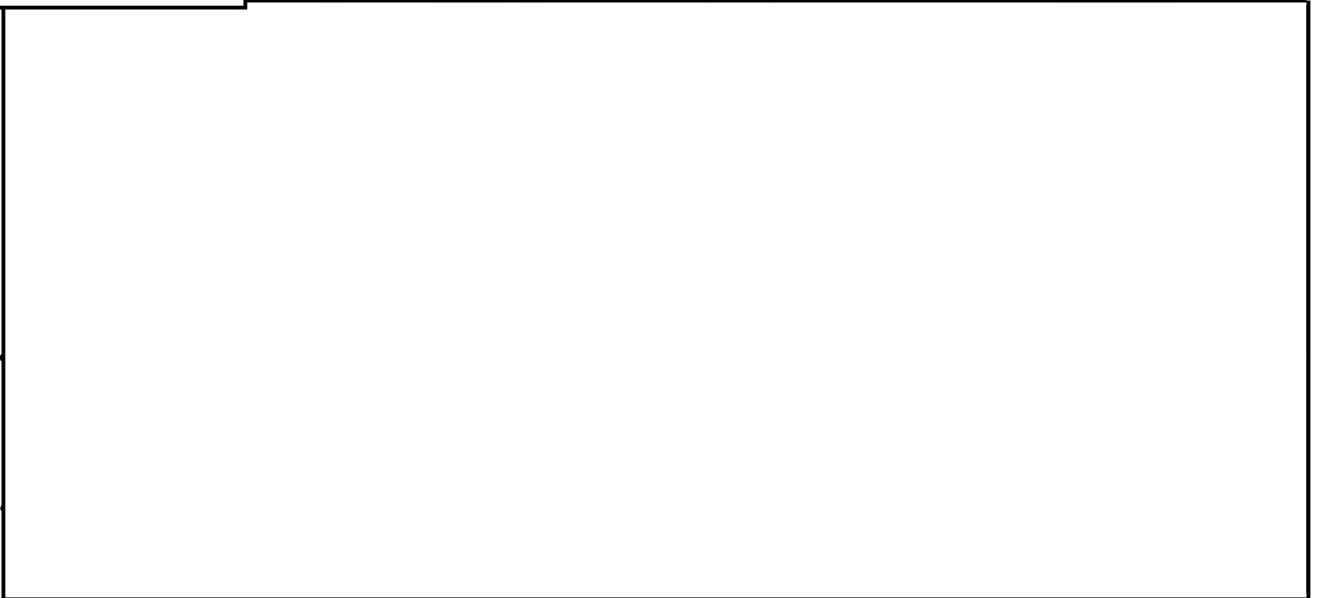


b4
b7E



b5
b6
b7C
b7E

[redacted] provided a presentation [redacted]



[Redacted]

b7E

[Redacted]

[Redacted]

FBI

• [Redacted] provided an overview

[Redacted]

b6
b7C
b7E

[Redacted]

[Redacted]

b7E

• [Redacted]

b6
b7C
b7E

• [Redacted]

• [Redacted]

b7E

[Redacted]

Town Hall Meeting

[Redacted]

OTD, FBI

• [Redacted] provided the

[Redacted]

b6
b7C
b7E

• [Redacted]

• [Redacted]

[REDACTED]

b7E

○

○

○

• [REDACTED]

○

○

○

b6
b7C
b7E

National Computer Forensics Institute

[REDACTED] *Director NCFI, USSS*

b6 Per USSS

b7C

- [REDACTED] provided information on training opportunities related to computer forensics and digital handling techniques for State and local law enforcement agencies, prosecutors, and judges at the National Computer Forensics Institute (NCFI) facility.
- Established in 2007, the NCFI was founded as a partnership among the United States Secret Service (USSS), the Alabama District Attorneys Association, the State of Alabama, and the city of Hoover, AL. The courses are based on the USSS electronic crimes training model.
- The mission of the NCFI is to provide state and local law enforcement, prosecutors and judicial officials a national standard of training in electronic crimes investigations, network intrusion response, computer forensics and high tech crime prosecution.
- Since its opening, the NCFI has trained and equipped 1,925 State and local officials, including 1,314 State and local police officials, 456 prosecutors and 165 judges from all 50 states and three U.S. Territories. These NCFI graduates represent over 1,000 State and local government agencies nationwide.
- Advantages for State and local Agencies
 - No Tuition. All travel costs, hotel, and per diem are covered by the NCFI.
 - No Equipment Costs. Students who attend the forensics and Network Intrusion courses are issued all of hardware software and licenses necessary to conduct these investigations.
 - Example: A Basic Computer Evidence Recovery Training (BCERT) trained officer will return to their department trained and equipped; giving their department its own computer forensics capability.
 - Membership within the US Secret Service Electronic Crimes Task Force (ECTF) Network
- NCFI Courses
 - Advanced Forensics Training (AFT)
 - Basic Investigation of Computer and Electronic Crimes Program (BICEP)
 - Basic Computer Evidence Recovery Training (BCERT)
 - Basic Network Investigation Training (BNIT)

- Cyber Analyst Crash Course
 - Network Intrusion Response Program (NITRO)
 - Mobile Device Data Recovery (MDDR)
 - Online Social Networking (OSN)
 - Computer Forensics in Court – Prosecutors (CFC-P)
 - Computer Forensics in Court – Judges (CFC-J)
 - Mobile Devices in Court – Prosecutors (MDP)
 - Point of Sales (POS)
- NCFI courses are in high demand. For every available training slot, the NCFI receives five applications.

b6
b7C
b7E

FBI

b7E

National Domestic Communications Assistance Center (NDCAC) Tour

The scheduled tour did not take place due to inclement weather closing the Federal Government on March 6, 2013.

UNCLASSIFIED// ~~LAW ENFORCEMENT SENSITIVE~~

LAW ENFORCEMENT TECHNICAL FORUM

Fredericksburg, Virginia

March 05 - 06, 2013



Tuesday, 03/05/13

Day One -- LETF

8:30 a.m. - 9:00 a.m.

Registration

9:00 a.m. - 9:15 a.m.

Administrative Matters / Welcome

SSA [REDACTED] CIU, CIS, OTD, FBI

SC William Searcy, CIS, OTD, FBI

UC [REDACTED] OTD, FBI

b6
b7C

9:15 a.m. - 10:00 a.m.

National Domestic Communications Assistance Center
(NDCAC)

UC [REDACTED] OTD, FBI

SSA [REDACTED] OTD, FBI

10:00 a.m. - 10:15 a.m.

BREAK

10:15 a.m. - 11:30 a.m.

Technology Trends

Steve Stoner, DOD

11:30 a.m. - Noon



b6
b7C
b7E

Noon - 1:00 p.m.

LUNCH

1:00 p.m. - 2:45 p.m.



b5
b6
b7C

2:45 p.m. - 3:15 p.m.



CIS, OTD, FBI

b6
b7C
b7E

UNCLASSIFIED// ~~LAW ENFORCEMENT SENSITIVE~~

UNCLASSIFIED// ~~LAW ENFORCEMENT SENSITIVE~~

3:15 p.m. – 3:30 p.m. **BREAK**

3:30 p.m. – 4:15 p.m. [redacted] **Town Hall Meeting**
[redacted] *CIS, OTD, FBI*

b6
b7C
b7E

4:15 p.m. – 5:00 p.m. **National Computer Forensics Institute**
[redacted] *Director NCFI, USSS*

b6 Per USSS
b7C

Wednesday, 03/06/13 Day Two -- LETF

8:30 a.m. – 9:30 a.m. **Regional Computer Forensic Lab (RCFL) Unit**
UC [redacted] *OTD, FBI*

b6
b7C
b7E

9:30 a.m. – 10:30 a.m. [redacted]
SSA [redacted] *FBI*

10:30 a.m. - Noon **National Domestic Communications Assistance Center
(NDCAC) Tour**

DAD Tony DiClemente, OTD, FBI
SSA [redacted] *NDCAC* [redacted] *OTD, FBI*

UNCLASSIFIED// ~~LAW ENFORCEMENT SENSITIVE~~